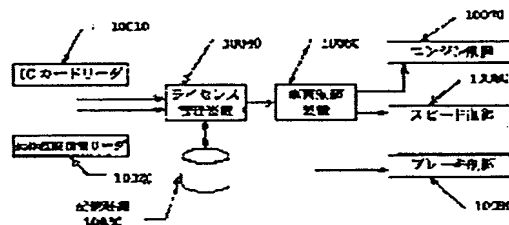


(11)Publication number : 2000-311220
(43)Date of publication of application : 07.11.2000

(71)Applicant : HITACHI LTD
(72)Inventor : SHIMIZU HIROSHI
KOMATA TAKASHI
MATSUMOTO KENJI

SOLUTION: An IC card reader 10010 exists in a vehicle and a driver inserts a self-IC card into the IC card reader 10010 when he or she drives the vehicle. A human body certification information reader 10020 reads human body certification information showing ID of a human himself (herself) such as the fingerprint or the iris/retina of the driver seated on a driving seat. A license managing device 10040 compares processor information of a license which is read from the IC card with human body recognition information of the driver seated on the driving seat and judges whether they are same or not. When the driver seated on the driving seat is judged to be the person himself (herself) having qualification for driving the vehicle, the license managing device 10040 sends a message showing operation permission to a vehicle controller 10060.



| | |
|---|------------|
| [Date of request for examination] | 22.02.2005 |
| [Date of sending the examiner's decision of rejection] | |
| [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration] | |
| [Date of final disposal for application] | |
| [Patent number] | |

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-311220

(P2000-311220A)

(43)公開日 平成12年11月7日(2000.11.7)

| (51)Int.Cl. ⁷ | 識別記号 | F I | テーマコード(参考) |
|--------------------------|-------|---------------|-------------------|
| G 0 6 K 17/00 | | G 0 6 K 17/00 | T 2 C 0 0 5 |
| B 4 2 D 15/10 | 5 2 1 | B 4 2 D 15/10 | 5 2 1 3 E 0 4 4 |
| G 0 6 T 7/00 | | G 0 6 F 15/62 | 4 6 5 K 5 B 0 3 5 |
| G 0 6 K 19/00 | | G 0 6 K 19/00 | T 5 B 0 4 3 |
| 19/10 | | | S 5 B 0 5 8 |

審査請求 未請求 請求項の数45 O L (全 14 頁) 最終頁に続く

(21)出願番号 特願平11-122395

(22)出願日 平成11年4月28日(1999.4.28)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 清水 宏

神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所デジタルメディア開発本部内

(72)発明者 小俣 隆

神奈川県横浜市戸塚区吉田町292番地 株式会社日立製作所デジタルメディア開発本部内

(74)代理人 100078134

弁理士 武 顕次郎

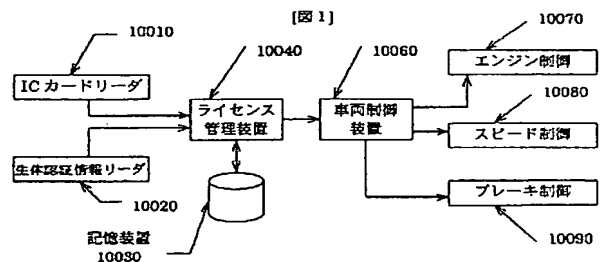
最終頁に続く

(54)【発明の名称】 機器操作権管理システムおよび機器操作権管理端末およびICチップおよびICチップケース

(57)【要約】

【課題】 機器を操作するライセンスとその所有者が同一であることを認証することで、確実な機器操作者の管理を行うようにすること。

【解決手段】 免許証としてメモリチップ等を搭載したICカードなどを用い、自動車に、ICカードまたは同等の機能を有する免許証を挿入する端末を設けると共に、乗車した運転手の指紋・虹彩等の生体認証情報を検知する生体認証情報検出手段を設け、また、ICカードまたは同等の機能を有する免許証のメモリに、免許証の所有者の生体認証情報を表わす情報を記載する。そして例えば、運転者の生体認証情報と免許証記載の生体認証情報との照合が一致し、かつ免許証の内容が運転する自動車に合わない限り、運転を不可能とする。



【特許請求の範囲】

【請求項 1】 機器を取り扱う権利を表示する許可表示手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、前記許可表示手段に記載されている権利者と、機器を操作する操作者との一致を、操作者の生体認証情報を用いて確認することを特徴とする機器操作権管理システム。

【請求項 2】 請求項 1 に記載の機器操作権管理システムにおいて、

前記許可表示手段は、メモリもしくは CPU を有する IC チップを搭載していることを特徴とする機器操作権管理システム。

【請求項 3】 請求項 1 もしくは 2 に記載の機器操作権管理システムにおいて、前記生体認証情報は、指紋情報であることを特徴とする機器操作権管理システム。

【請求項 4】 請求項 3 に記載の機器操作権管理システムにおいて、

前記生体認証情報を検出するセンサを、機器を最初に作動させるスイッチ上に設けたことを特徴とする機器操作権管理システム。

【請求項 5】 請求項 1 もしくは 2 に記載の機器操作権管理システムにおいて、

前記生体認証情報は、網膜もしくは虹彩形状を示す情報であることを特徴とする機器操作権管理システム。

【請求項 6】 請求項 5 に記載の機器操作権管理システムにおいて、

前記生体認証情報を検出するセンサを、機器のステータス情報を表示するパネルに設置することを特徴とする機器操作権管理システム。

【請求項 7】 請求項 1 もしくは 2 に記載の機器操作権管理システムにおいて、

操作機器内に、前記許可表示手段の読み取り装置と、前記生体認証情報を検出するセンサとを設置することを特徴とする機器操作権管理システム。

【請求項 8】 請求項 1 もしくは 2 に記載の機器操作権管理システムにおいて、

操作機器とは別体の携帯端末装置に、前記許可表示手段の読み取り装置と、前記生体認証情報を検出するセンサとを設置することを特徴とする機器操作権管理システム。

【請求項 9】 請求項 1 もしくは 2 に記載の機器操作権管理システムにおいて、

操作機器内に、前記生体認証情報を記憶する記憶装置を有することを特徴とする機器操作権管理システム。

【請求項 10】 請求項 2 に記載の機器操作権管理システムにおいて、前記許可表示手段に搭載した IC チップに、前記生体認証情報を記憶することを特徴とする機器操作権管理システム。

【請求項 11】 請求項 10 に記載の機器操作権管理システムにおいて、

記憶している前記生体認証情報は複数種であり、操作する機器が、照合に使用する前記生体認証情報をそれぞれ自由に選択可能であることを特徴とする機器操作権管理システム。

【請求項 12】 請求項 1 もしくは 2 に記載の機器操作権管理システムにおいて、

前記生体認証情報の認証精度を、操作する機器の種類に応じて変化させることを特徴とする機器操作権管理システム。

【請求項 13】 請求項 1 もしくは 2 に記載の機器操作権管理システムにおいて、

前記生体認証情報の認証を、機器の起動前毎に行うことを特徴とする機器操作権管理システム。

【請求項 14】 請求項 1 もしくは 2 に記載の機器操作権管理システムにおいて、

前記生体認証情報の認証を、機器の起動後に一定時間間隔で行うことを特徴とする機器操作権管理システム。

【請求項 15】 請求項 1 もしくは 2 に記載の機器操作権管理システムにおいて、

前記生体認証情報の認証を、機器に搭乗する扉の開閉時毎に行うことを特徴とする機器操作権管理システム。

【請求項 16】 請求項 1 もしくは 2 に記載の機器操作権管理システムにおいて、

前記生体認証情報の認証を、機器の動作終了時毎に行うことを特徴とする機器操作権管理システム。

【請求項 17】 機器を取り扱う権利を表示する許可表示手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、

機器の操作許可を得ている者に発行した前記許可表示手段に記載されている ID 番号を、少なくとも 1 つ以上記憶する記憶装置を有することを特徴とする機器操作権管理システム。

【請求項 18】 請求項 17 に記載の機器操作権管理システムにおいて、

前記許可表示手段は紙等の非電子手段により構成され、前記 ID 番号は該許可表示手段上に光学的に読み取り可能な形態で記載されており、前記機器制御手段は、前記許可表示手段に記載された ID 番号を読み取る読み取り手段を有することを特徴とする機器操作権管理システム。

【請求項 19】 請求項 17 もしくは 18 に記載の機器操作権管理システムにおいて、

前記許可表示手段に記載された ID 番号が、前記機器制御手段内の記憶装置に記憶されている ID 番号と一致しない限り、機器の操作を不可能とすることを特徴とする機器操作権管理システム。

【請求項 20】 請求項 17 から 19 の何れか 1 つに記載の機器操作権管理システムにおいて、

前記機器制御手段内の記憶装置に記憶されている ID 番号と一致した ID 番号の前記許可表示手段を有する者に、前記記憶装置に新たな ID 番号を追加もしくは変更もしくは削除する手順の操作許可を与えることを特徴とする機器操作権管理システム。

【請求項 21】 機器を取り扱う権利を表示する許可表示手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、前記許可表示手段に記載されている操作可能機器情報を読み取る読み取り手段を有し、前記機器制御手段は、前記許可表示手段に記載されている前記操作可能機器情報が自身の機器と一致しているかの判断を行い、一致していれば機器の操作を可能とすることを特徴とする機器操作権管理システム。

【請求項 22】 請求項 21 に記載の機器操作権管理システムにおいて、前記許可表示手段は紙等の非電子手段により構成され、前記操作可能機器情報は該許可表示手段上に光学的に読み取り可能な形態で記載されており、前記機器制御手段は、前記許可表示手段に記載された操作可能機器情報を読み取る光学的読み取り手段を有することを特徴とする機器操作権管理システム。

【請求項 23】 請求項 21 に記載の機器操作権管理システムにおいて、前記操作可能機器情報に従って、機器の操作可能範囲を変更することを特徴とする機器操作権管理システム。

【請求項 24】 請求項 2 に記載の機器操作権管理システムにおいて、前記許可表示手段に搭載した IC チップは、複数のアプリケーションの実行が可能な CPU カードであることを特徴とする機器操作権管理システム。

【請求項 25】 請求項 24 に記載の機器操作権管理システムにおいて、前記 CPU カードは、電子マネー機能を含むカードであることを特徴とする機器操作権管理システム。

【請求項 26】 請求項 2 もしくは 24 に記載の機器操作権管理システムにおいて、前記許可表示手段に搭載した IC チップは、機器が搭乗および移動可能な機器である場合に、機器の移動に伴う位置や、該位置に到達した時刻等の情報を記録することが可能であることを特徴とする機器操作権管理システム。

【請求項 27】 請求項 2 もしくは 24 に記載の機器操作権管理システムにおいて、機器の使用におけるルール違反等に対する罰則として、機器の使用制限を行うことを特徴とする機器操作権管理システム。

【請求項 28】 請求項 27 に記載の機器操作権管理システムにおいて、前記罰則は機器操作の一定期間の禁止を含み、時間軸に

沿って、機器の使用許可および使用禁止の設定を複数回設定することが可能であることを特徴とする機器操作権管理システム。

【請求項 29】 請求項 27 もしくは 28 に記載の機器操作権管理システムにおいて、前記罰則は機器操作における機能の制限を含み、時間軸に沿って、機器の使用許可および禁止を含めて、機器の使用機能制限を複数回にわたって設定することが可能であることを特徴とする機器操作権管理システム。

【請求項 30】 請求項 27 から 29 の何れか 1 つに記載の機器操作権管理システムにおいて、前記罰則施行時期を管理する時計は、保証された時刻情報以外の情報により、機器の使用者が改変することを不可能とすることを特徴とする機器操作権管理システム。

【請求項 31】 機器操作許可情報を有する IC チップであって、該 IC チップには、機器操作許可を有する IC カードの所有者の ID 番号および操作可能機器情報が記載されていることを特徴とする IC チップ。

【請求項 32】 請求項 31 に記載の IC チップにおいて、前記 IC チップには、機器操作許可を有する IC カードの所有者の指紋や網膜・虹彩等の生体認証情報が記載されていることを特徴とする IC チップ。

【請求項 33】 請求項 31 に記載の IC チップにおいて、前記 IC チップには、電子マネー機能も併せて含むことを特徴とする IC チップ。

【請求項 34】 請求項 31 に記載の IC チップにおいて、前記 IC チップには、機器が搭乗および移動可能な機器である場合に、機器の移動に伴う位置や、該位置に到達した時刻等の情報が記録されることを特徴とする IC チップ。

【請求項 35】 請求項 31 に記載の IC チップにおいて、前記 IC チップには、機器の使用におけるルール違反等に対する罰則として、機器操作の一定期間の禁止を含み、時間軸に沿って、機器の使用許可および使用禁止の設定を複数回設定することが可能な情報を含むことを特徴とする IC チップ。

【請求項 36】 請求項 31 に記載の IC チップにおいて、IC チップには、機器の使用におけるルール違反等に対する罰則として、機能の制限を含み、時間軸に沿って機器の使用許可および禁止を含めて、機器の使用機能制限を複数回にわたって設定することが可能な情報を含むことを特徴とする IC チップ。

【請求項 37】 請求項 31 から 36 の何れか 1 つに記載の IC チップにおいて、

前記 IC チップは、IC カード内の IC チップであることを特徴とする IC チップ。

【請求項 38】 請求項 31 から 36 の何れか 1 つに記載の IC チップにおいて、
前記 IC チップは、機器を始動する鍵に内蔵されることを特徴とする IC チップ。

【請求項 39】 請求項 31 から 36 の何れか 1 つに記載の IC チップにおいて、
前記 IC チップには、前記罰則施行時期を管理する時計を内蔵し、この時計は保証された時刻情報以外の情報により、機器の使用者が改変することを不可能とすることを特徴とする IC チップ。

【請求項 40】 請求項 39 に記載の IC チップにおいて、
前記時計を駆動する電池の寿命は、機器操作許可の期限と略等しい寿命であることを特徴とする IC チップ。

【請求項 41】 機器を取り扱う権利を表示する許可表示手段に記載した情報を読み取る読み取り手段と、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理端末において、
機器の操作許可を得ている者に発行した前記許可表示手段に記載されている ID 番号を少なくとも 1 つ以上記憶する記憶装置を有することを特徴とする機器操作権管理端末。

【請求項 42】 請求項 41 に記載の機器操作権管理端末において、
前記機器操作権管理端末内の前記記憶装置に記憶されている ID 番号と一致した ID 番号の前記許可表示手段を有する者に、前記記憶装置に新たな ID 番号を追加もしくは変更もしくは削除する手順の操作許可を与えることを特徴とする機器操作権管理端末。

【請求項 43】 半導体メモリもしくは CPU で構成された IC チップを内蔵した IC チップケースであって、
IC カード内の前記 IC チップは電気的な接点部分を除いて絶縁体にて封印されており、前記 IC チップの電気的な接点の露出部のみを除くように、前記絶縁体の外面全体を導電体で覆った形状で構成されることを特徴とする IC チップケース。

【請求項 44】 請求項 43 に記載の IC チップケースにおいて、
前記 IC チップの電気的な接点の露出部と、前記導電体を結ぶ直線の間には、前記絶縁体が必ず存在することを特徴とする IC チップケース。

【請求項 45】 半導体メモリもしくは CPU で構成された IC チップを内蔵する、機器を取り扱う権利を表示する許可表示手段と、該表示許可手段と接続可能なインタフェースを有する、機器の動作可否を制御する機器制御手段とを具備した機器操作権管理システムにおいて、
前記 IC チップは、情報の暗号化・復号化を行う機能を有し、前記インタフェースには、前記 IC チップと同等

の機能を有する IC チップもしくはアプリケーションソフトウェアを搭載し、前記許可表示手段に内蔵した IC チップと、前記インタフェースとの間の通信を、暗号化された信号により行うことを特徴とする機器操作権管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、機器の操作の可否を管理・制御する機器操作権管理システムにかかわる技術に関し、特に、自動車の免許証等に代表されるライセンスカード形態の機器操作権を表記する機能を有するデバイスと、同デバイスと連携して機器操作者本人であることを生体認証情報を用いて照合する機能などを有する、機器操作権管理システムにかかわる技術に関するものである。

【0002】

【従来の技術】機器を操作する権利を有することを証明する証明書を発行し、その証明書を保有する者のみが、当該機器の操作を可能とするような、機器操作権管理方法は、各所で利用されている。例えば運転免許証の場合、免許証を持つ者のみが自動車を運転する権利を有し、警察官による運転免許証の提示指示が出たときは、速やかにこれに従い、従えない場合は罰則を科すシステムとして実運用されている。

【0003】しかし、自動車の運転免許証は、警察官の提示指示があるとき以外は、その効力を発揮することなく、免許証を持っていなくても、実際には自動車の運転は可能であり、機器操作権を確実に管理するには至っていない。

【0004】この問題を解決するために、特開平 6-87285 号公報に開示された技術では、運転免許証として IC カードを用い、この IC カードには、ドライバーの ID 等の免許証に記載されている事項を電子情報として記入し、自動車にはこの情報を読み取る端末を設け、有効な免許証でない限り、この自動車の運転が出来ないようにし、且つ、IC カード内に運行記録を記入して、後に各ドライバーの稼動状況を集計する方式が記載されている。

【0005】

【発明が解決しようとする課題】上記した先願公報に開示された技術においては、警察官に提示するとき以外に効力を持たなかった免許証を、自動車が常に判別することで、自動車を運転する権利を示す免許証としての確実な運用が可能になり、併せて IC カードのメモリ機能の特徴を生かして、運行状況のログを取り、最適な運行計画に反映させることも可能になる。

【0006】しかし、前記先願公報に開示された技術では、下記に示すような問題があり、これらの点への配慮がなされていない。

【0007】①まず、前記先願公報では、自動車に IC

カード免許証を挿入した者が、本当に免許証の所有者かどうかを確認することに関しては、何らの配慮も払われていない。したがって、免許証の交付を受けた者と運転者とが同一人でない場合でも、すなわち、実際には免許が与えられていない者でも、免許証を所持さえしていれば、運転が可能になる。

【0008】②また、前記先願公報では、交通違反等により免許証を失効したときの対応については、交通事故や交通違反時に、データ管理装置を用いて、免許証内に事故や違反データを書き込みすることや、出頭命令書や反則金納付書を発行することや、あるいは、免許停止・失効中には、免許証を自動車の端末に差し込んでエンジンがかからないようにすることに関する記述はあるものの、これらは現行の免許証運用方法にのっとったものであって、ICカードを利用することにより初めて得られるメリットを、罰則に適用した検討についてはなされていない。

【0009】③また、前記先願公報では、自動車のICカード端末に、この自動車を運転することが出来る運転手のIDリストを有し、このIDと一致する運転手のみが運転できる旨は記載されてはいるものの、免許証の種類と運転可能な自動車の種類及び運転モード種類との連携については、その検討が全くなされていない。

【0010】④さらに、前記先願公報では、ICカード内容の違法な変更に対して防護を施すことに関しても、何らの配慮も払われていない。

【0011】本発明は上記の点に鑑みなされたもので、その目的とするところは、機器を操作するライセンスとその所有者が同一であることを、確実に認証可能とすることにある。また、本発明の目的とするところは、操作の違反を行った場合の操作制限について、木目細かく、より実質に沿った処置が可能にようにすることにある。また、本発明の目的とするところは、ライセンスのレベルにより機器操作の制限を細かく設定することを可能とし、以って、確実な機器操作者の管理と、誤操作を防止できるようにすることにある。また、本発明の目的とするところは、CPUカードを用いることで、物理的な破壊以外のソフトウェアによるカードの破壊を防止することにある。

【0012】

【課題を解決するための手段】上記した目的を達成するために、本発明では、例えば以下のような手段を用いる。

【0013】(1) 自動車のICカードまたは同等の機能を有する免許証を挿入する端末を設けると共に、乗車した運転手の指紋や虹彩等の生体認証情報を検知する生体認証情報の検出手段を設け、前記ICカードまたは同等の機能を有する免許証のメモリに、免許証の所有者の生体認証情報を表わす情報を記載する。

【0014】(2) 特に自動車の場合は、通行中に違反

を受けて、前記先願公報に記載のような処理を受けると、違反を起こした場所で自動車の運転が不可能になり、車の移動が不可能となってしまう。そこで、ICカード内に、違反時の自動車の運転許可パターンを細かく時間軸に沿って設定することで、例えば、実際の免許停止処分の発行を2日後に設定し、自動車の端末もその指示に沿って動作する。

【0015】(3) ライセンスのレベルにより、運転する車の動作モードを規定する。例えば、教習所等の専用コースや駐車場において、速度10km/h未満の走行のみが行えるライセンスの設定を行い、自動車の端末もその指示に従って動作する。

【0016】(4) CPUカードを用いることで、物理的な破壊以外のソフトウェアによるカードの破壊を防止しつつ、暗号処理の必要のないデータの簡単な読み出しを可能とする。具体的には、上記(2)、(3)記載の免許停止処分の発行日程やライセンスレベルを、外部に特別な暗号処理チップを用いることなく読み出せ、且つその情報の破壊・改変を防止する。

【0017】

【発明の実施の形態】以下、本発明の実施の形態を、図面を用いて説明する。

【0018】図1は、本発明の第1実施形態に係る機器操作権管理システムの構成を示すブロック図であり、本実施形態は、自動車における機器操作権管理システムへの適用例である。本システムは、機器（ここでは自動車）の動作の可否を制御する機器制御機能をもつ装置と、機器を取り扱う権利（ここでは運転免許であり、例えば、教習所内などの限定されたエリアのみでの運転を許可するものを含むものとする）を示す情報をもつ許可表示手段としてのICカードとを、少なくとも含むものとなっている。

【0019】自動車にはICカードリーダ10010があり、ドライバーは自動車を運転する際に、自身のICカードをICカードリーダ10010に差し込む。生体認証情報リーダ10020は、運転席に座ったドライバーの指紋もしくは虹彩・網膜などの人間自身のIDを示す生体認証情報を読み取る。ライセンス管理装置10040は、前記ICカードリーダ10010によってICカードから読取られた、該当免許証の所有者の情報と、同じく前記生体認証情報リーダ10020によって読み取られた、運転席に座ったドライバーの生体認証情報とを比較し、同一であるかどうかの判断を行う。

【0020】記憶装置10030は、例えばこの車両を運転してもよいドライバーを限定するときに、そのドライバーIDを記憶する。差し込まれたICカードのドライバーIDが、この記憶装置10030に記憶されたドライバーIDと一致しないときは、後述する車両制御装置10060によりエンジン始動を抑制する。

【0021】ライセンス管理装置10040が、差し込まれ

た IC カードからの情報と生体認証情報リーダ 10020 からの情報とにより、運転席に座ったドライバーが確かにこの自動車を運転する資格を有する本人と判断したとき、ライセンス管理装置 10040 は、車両制御装置 10060 に動作許可を示すメッセージを送る。

【0022】車両制御装置 10060 は、この許可メッセージに従って、エンジン始動の可否を含めてエンジンの制御を行うエンジン制御装置 10070 や、自動車の走行速度のリミッターを制御するスピード制御装置 10080 や、ABS (Antilock Brake System) の動作、レベルを設定するブレーキ制御装置 10090 に、それぞれ動作許可指示を送る。これによりエンジンの始動が可能になり、またドライバーの資格レベルに従った最高速度の設定、さらに、現行の免許証制度では存在しないがドライバーの技量に見合った形で ABS の ON/OFF 制御を行う。

【0023】図 2 は、本実施形態の機器操作権管理システムにおける、自動車の操縦席近傍へのシステム配置の 1 例を示した説明図である。

【0024】20000 はコックピットである。運転席右に IC カード挿入口 20020 があり、この自動車を運転するドライバーは、自身の免許証である IC カードをこの挿入口 20020 に挿入する。次に、指紋読み取り部兼エンジン始動ボタン 20030 を押すことで、ドライバーの指紋を読み取り、先の IC カードに記載したドライバーの生体認証情報との認証を行う。そして、紋読み取り部兼エンジン始動ボタン 20030 を押した人が、確かに IC カードの示す本人であることを認識して、初めてエンジンの始動が行える。

【0025】このとき、記憶装置 20050 に、この自動車を操縦してもよいドライバーの ID リストを持つことにより、挿入した IC カードの ID との照合を行い、図 1 の説明と同様に、操縦許可のないドライバーでは、自動車のエンジン始動を含む操作が出来ないようにして、盗難防止等のセキュリティを確保することが出来る。

【0026】生体認証情報の確認手法としては、スピードメーター位置に網膜・虹彩センサ 20010 を設ける方法もある。この場合、ドライバーが運転席に座らない限りは、このセンサを用いて検出することが出来ないのので、例えば先の指紋読み取り部兼エンジン始動ボタン 20030 を、IC カード (免許証) を交付された本人が助手席から押して、免許証がない人が運転席に座って運転するようなことが、不可能になる。ここで、スピードメーターはドライバーの視線が必ず行くところであり、且つドライバーシートは頭の位置がほぼ固定されるので、網膜・虹彩センサ 20010 を設置するのに適している。

【0027】また、ここで免許証として利用するデバイスは、IC カードであり、電子マネー等で使用するマルチアプリケーション対応の IC カードである。これにより、同じ IC カード内に、電子マネーや電子クレジット等のアプリケーションを同居させることが出来、自動車

から料金自動支払いシステム 20040 へのアクセスによって、高速道路の自動料金支払いや、ドライブスルーやガソリンスタンド等の必ず自動車に乗車している条件下で買物を行うシステムへの対応を行うことも出来る。

【0028】さらに、ここで使用する免許証が IC カードを用いずに、従来の印刷物による免許証を利用しても、カード挿入口に免許証を挿入して、ID 番号等をイメージスキャナで読み取ることで、この自動車の操縦許可を得ているドライバーの免許証かどうかの判断を行うことが出来る。さらに記憶装置 10030 に、ドライバーの生体認証情報を記録しておくことで、IC カードを用いなくても、従来の免許証システムで、免許証と生体認証情報によるドライバー本人との照合を行うことも可能であり、IC カードではなく従来の免許証システムをそのまま用いても、本発明の機能を実現することが出来る。

【0029】図 3 は、本実施形態の機器操作権管理システムにおいて用いる IC カードの内部構成 (IC カードに搭載した IC チップの内部構成) の 1 例を示す説明図である。

【0030】IC カード 30000 に搭載した IC チップ 30005 は、MF 30010 (Master File) をルートとして、その下位に複数の DF (Dedicated File) を有し、DF 1 (30020) は免許証、DF 2 (30060) は例えば電子マネーに用いられている。DF 1 (30020) の下には複数の EF (Elementary File) があり、電子免許証に関連する情報が記載されている。EF 1 (30030) には、免許証 ID 番号と、生体認証情報を示す指紋情報や虹彩情報などがある。この場合、生体認証情報は複数種類あってもよく、自動車の端末に装着された生体認証情報リーダ 10020 が、例えば指紋スキャナであった場合は、指紋情報を用い、虹彩センサであるならば、虹彩情報を用いればよい。EF 2 (30040) には、この免許証のライセンス種類やレベルが、そして EF 3 (30050) には、違反履歴が記載される。CPU カードは、DF や EF がプログラムになっており、外部から特定のコマンドを入力するときのみ、生体認証情報を読み出したり、違反履歴を書き換えたりすることが出来る。この特定のコマンドは、専用のソフトや後述する専用のチップのみが行い、これによりカードの内部情報の機密を保ち、改変を防止することが出来る。

【0031】また、ここでカード内に時計 30070 を設け、前記生体認証情報や違反履歴と同様に、専用のソフトやチップを介さない限り、この時計の日付・時刻を改変出来ない仕掛けとすることで、図 4 にて後述する、違反時の罰則発行を日付に従って施行する際に、故意に時計を狂わせて罰則発行を免れるような行為を完全に防止することが出来る。カード上で単体で動作する時計のため、当然狂いが生じるが、これはカードを車載の端末に挿入したときに、専用のソフトもしくはチップが GPS 等の確実に信頼できる時計により確認した正しい時刻を

用いて、カード内の時計の狂いを修正する。この時刻の修正は、自動車に搭載した端末に限らず、図2に示した料金自動支払い時の通信において行ってもよく、また自動車に関係なく、電子マネー端末と連携して、電子マネーや電子クレジットによる買物を行った際に、端末から時計の修正を随時行ってもよい。また、ICカード内に設置された時計は、ICカードの駆動電源を外部から与えられなくても動作する必要がある、薄型電池をICカード内に内蔵する。この電池の寿命は、基本的に免許の許可期限以上の寿命とするが、場合によっては、免許の許可期限と略同程度の寿命を持つようにしてもよい。時計の駆動以外ではこの電池は一切使用しないので、使用条件により寿命が短くなるという現象は起きず、正確に寿命の設定をすることが可能である。

【0032】図4は、本実施形態における、違反時の罰則処理パターン1例を示す表図である。

【0033】罰則処理のパターンとして、本実施形態では、自動車を運転する際の動作モードを、(1)エンジン始動のみ、(2)10km/h未満の走行、(3)通常走行可能の3つに分類した。例えば無違反の場合は、当然ながらこの3つの動作モードをすべて使うことが可能である。

【0034】まず、従来の免許停止に相当するスピード違反について示す。従来の免許証では、スピード違反による罰則すなわち免許停止は即時発行するが、例えば旅行途中でスピード違反をした場合には、そのまま乗って帰ることになり、さらに警察に見つからなければ、そのまま乗り続けることも現実には可能となってしまう。そこで、例えばICカード等による電子情報として違反情報を記載し、自動車にこれに対応する端末を設け、免許停止を即時発行した場合は、その場で例えば半年間のあいだ、自動車を動かすことが出来なくなり、道の真ん中で車を置き去りにするという現象が発生する。本実施形態では、スピード違反をした後、その罰則の発行を違反時から例えば2日後からと設定し、その間に自動車を自宅に持ち帰ったり、貸出し元に返却したりする。その上で実際の罰則が発行されて、この免許証では運転が出来ないような処理をすることが出来る。

【0035】また、即時免許停止が必要なほど異常なスピード違反を行った場合、少なくとも高速道路のサービスエリア上の道端から、駐車エリアまでは車の移動が出来るように、10km/h以下の走行のみを例えば2日間の一定期間だけ可能とし、一般道路の通常走行の禁止は即時発行する。

【0036】また、酒気帯び運転による免許停止発行の場合は、少なくとも摘発時点では車の走行は即時やめさせる必要がある。10km/h以下の走行は勿論、自動車のエンジン始動も不可能とする。これは摘発されたドライバーが酔いから醒めるまでの期間として、例えば6時間だけ完全な運転禁止とし、その後、前記したス

ピード違反と同様に2日間だけ通常走行を可能として、自宅に車を持ち帰った後、免許停止が初めて発行される。この期間はドライバーの自宅までの距離や情状酌量に応じて、摘発した担当者が決定することが出来る。

【0037】なお、ICカードに書き込む罰則による制限事項は、時間軸に沿って、使用許可、使用禁止、使用機能制限などを複数回にわたって設定可能となっている。

【0038】本実施形態における罰則発行の時期・時刻は、ある基準となる時計に従って施行されるが、例えば通常の自動車に搭載された時計を用いた場合、ドライバーが勝手にその時計を変更し、例えば時計を半年進めてしまえば、すでに処分期間は過ぎているので、勝手に運転をすることが可能となってしまう。これを防ぐために、図3に示したように、外部から勝手に時刻の変更を行えないような時計をICカード内に持ったり、同様な機能、すなわちGPS等の確実に信頼できる時計により時刻の修正を行う以外は、任意の時刻設定がまったく出来ないような時計を、車載の端末に持たせてもよい。

【0039】図5は、本発明の第2実施形態に係る機器操作権管理システムにおける、ライセンス種類による動作モードの規定の1例を記述した表図である。本実施形態はヘリコプターの操縦を想定した例であり、正規ライセンスのパイロット、訓練生、そしてメカニックそれぞれのライセンスと、それぞれに対する動作モードを示している。

【0040】正規ライセンスのパイロットは、当然ながらエンジン始動、ホバリング、低速飛行、高速飛行のすべてを行うことが出来る。訓練生の場合は、エンジン始動から低速飛行までが行え、高速飛行への制限がある。具体的には、例えばメインローター回転面の角度を、パイロットの意志では一定以上傾けることが出来ないような制御を入れる。勿論ジャイロ等による自動姿勢制御はこの制限を受けずに、角度一杯まで倒すことが可能である。また、簡単な浮上試験が出来る資格を持つメカニック1級はエンジン始動及びホバリングまで可能とする。具体的には、極低速の前後左右移動までが可能な程度に、例えばメインローター回転面の角度の変更操作が不可能となるような制御を行う。整備資格のみを持つメカニック2級の場合はエンジン始動のみである。

【0041】このような制御の具体的な制限手法は、操縦する機器により異なるが、ICカード免許にライセンスのレベルを記載し、実際に操作する機器側で、そのライセンスでどこまで操作出来るかを設定することで、例えば自動車を運転する際、同じ仮免許証でも、一般道路と専用コース内で動作モードを変えるような制御が可能である。

【0042】図6は、本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順を示したフローチャートの第1例である。

10

20

30

40

50

【0043】まず、操作する機器に I D カードを挿入し（ステップ60010）、次に指紋の入力を行う（ステップ60020）。次に、ステップ60030にて、挿入した I D カードに記載された指紋情報と、入力した指紋情報の一致を判定して、指紋を入力した者が I D カードの所有者かどうかの判定を行う。判定が×であれば、運転不可の表示を行いつつ、I D カードの Eject を行う（ステップ60040）。照合結果が○であれば、エンジンスタートを行い（ステップ60050）、操縦する機器が自動車であれば、走行を行う（ステップ60060）。

【0044】ここで、例えば I D カードは前記した如く、メモリを持つ I C チップにより構成されるものだけではなく、現状使用されている印刷物の免許証の免許証番号等をイメージスキャナで読み取り、図1、図2で示した機器に搭載されている記憶装置から、該当免許証番号に対応した指紋情報を読み出して、操縦者が入力した指紋との一致判断を行ってもよく、この場合は、現行の印刷物免許証でも同等の機能を達成することが出来る。

【0045】図7は、本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順を示したフローチャートの第2例と第3例である。

【0046】図7の（a）は、I D カードと操縦する機器の種類の照合を行う場合のフローチャートである。まず、操縦者は機器に I D カードを挿入し（ステップ70010）、操縦する機器は挿入された I D カードからライセンス I D を読取る。そして、該当ライセンス I D が、本機器を操縦できるライセンスかどうかの判定を行い（ステップ70020）、操縦が出来ない場合は運転不可表示を行い、且つ I D カードの Eject を行う（ステップ70030）。照合結果が○であれば、エンジンスタートを行い（ステップ70040）、操縦する機器が自動車であれば、走行を行う（ステップ70050）。

【0047】ここで、例えば I D カードは前記した如く、メモリを持つ I C チップにより構成されるものだけではなく、現状使用されている印刷物の免許証の免許証番号及び記載されている操縦可能機器の種類をイメージスキャナで読み取り、本機器を操縦できるライセンスかどうかの判断を行ってもよく、この場合は、現行の印刷物免許証でも同等の機能を達成することが出来る。

【0048】図7の（b）は、図6と図7の（a）の両方の機能を実現した例を示すフローチャートである。すなわち、操縦者は機器に I D カードを挿入し（ステップ70010）、次に指紋の入力を行う（ステップ70060）。次に、ステップ70070にて、挿入した I D カードに記載された指紋情報と、入力した指紋情報の一致を判定して、指紋を入力した者が I D カードの所有者かどうかの判定を行う。判定が×であれば、運転不可の表示を行いつつ、I D カードの Eject を行う（ステップ70031）。照合結果が○であれば、挿入された I D カードから読み取ったライセンス I D が、本機器を操縦できるライセン

スかどうかの判定を行い（ステップ70021）、操縦が出来ない場合は運転不可表示を行い、且つ I D カードの Eject を行う（ステップ70032）。照合結果が○であれば、エンジンスタートを行い（ステップ70041）、操縦する機器が自動車であれば、走行を行う（ステップ70051）。

【0049】ここで、指紋照合とライセンス I D の照合順序は、どちらでも構わないが、例えば自動車において、指名手配者等のライセンス I D をネットワーク等で自動車に常受信している場合、この照合時点にて自動車は搭乗しているドライバーが犯罪者等であることを認識し、運転不可表示を行うと同時に、図示しない通信手段を用いて、犯罪者の存在を警察等に知らせるという仕掛けを実現することも出来る。この手順を一番最初に行うことで、確実な犯罪者の検知を行うことが可能となる。

【0050】なおまた、指紋照合などの生体認証情報の認証（照合）は、自動車等の乗り物の所定の扉の取っ手に指紋読み取りセンサを設けることなどにより、乗り物に搭乗する際の、扉の開閉操作と同時に行うようにしてもよい。

【0051】さらにまた、指紋や虹彩などの生体認証情報の認証（照合）は、自動車などの機器の起動前毎に行うだけでなく、機器の起動開始許可後に、一定時間毎に行うようにしたり、あるいは、機器の動作終了時毎に行うようにしてもよい。このようにすることで、機器の動作を立ち上げた後に、最初に認証した人物と異なる者が、途中で機器の運転や操縦などを交代したかどうかを監視することができる。そして、途中で運転や操縦などを交代した場合には、自動車等の機器がこの旨を警告したり、時と場合によるが警告後に機器の動作を徐々に停止させたり、あるいは、I C カードや機器の記憶装置に、不正交代したことの情報と交代後の人物の生体認証情報とを併せて記録したり、または、不正交代したことの情報と交代後の人物の生体認証情報とを外部に自動報知したりするような、仕組みとすることもできる。したがって、タクシーなどにおいて、悪意の乗客が車を乗っ取って運転した時などにおいて、大いにその効力を発揮する。

【0052】図8は、本発明による機器操作権管理システムにおいて適用可能な、I C カードリーダおよび生体認証情報リーダを装着してなる、機器の起動を行うためのリモコンの実施形態の例を示した説明図である。

【0053】図8の（a）に示したリモコンは、リモコンに I C カードリーダと生体認証情報リーダとしての指紋スキャナとを具備させることにより、前記した第1実施形態における機器制御機能をもつ車載の装置（端末装置）と同等の機能を持たせたものである。

【0054】リモコン本体には、指紋スキャナ兼スターボタン80020があり、利用者が I C カード80030を

差し込んで、ボタン80020 に指を乗せることで指紋のスキニングを行い、ICカード80030 内に記載した指紋情報とスキニングした利用者の指紋情報との照合を行って、照合が成立したときに初めて、赤外線／電波発射口80010 より、自動車のエンジンスタータートやドアロック解除等の信号を、赤外線もしくは電波によって発射する。

【0055】図8の(b)は、ICカードの機能をリモコンの内部に内蔵した例である。この例の場合、汎用の自動車の免許証とは異なる使用形態になるが、ある機器を動かそうとしたときに、その機器を動かす資格のある者の指紋情報を記憶しているので、他の者が機器を動かそうとしてもスタート出来ない。また、ICカードの差し込みがないのでカードの携帯による紛失を回避することも出来る。

【0056】図9は、本発明による機器操作権管理システムにおいて、機器の使用許可を出していない者に使用許可を出す方法例を示した説明図である。具体的な例として、ある自動車のオーナーが、その自動車を運転する権利を他の人に与えるための操作フローを、操作画面を元に説明する。

【0057】まず、図9の(a)の操作画面で示すように、自動車は他人への運転許可を与える人が、確かにその車のオーナーかどうかの判定をするために、オーナーにIDカードの挿入を促す。ここで、図示しない指紋等の生体認証情報の照合により、オーナー本人であることを確認する。

【0058】次に、図9の(b)に示す操作画面で、他人に与える運転許可モードを選択する。すなわち、

「1」を選択することで当日のみ、「2」を選択することで指定日付を指定する。そして、「3」を選択することで、例えば家族などの永久ライセンスを与える。この選択の後、図9の(a)と同様な操作画面にて、運転許可を与えるドライバーのIDカードの挿入を促し、運転許可の登録を行う。

【0059】図9の(c)の画面は、現在この車に既に登録されている運転可能ドライバーの一覧を表示したものを示す。ここで番号により選択を行うことで、図9の(d)の操作画面に示すように、運転許可モードの変更を行うことが出来る。

【0060】図10は、本発明による機器操作権管理システムにおいて、生体認証情報の認証の精度を操縦する機器によって変更するパターンの例を示した説明図である。生体認証情報の認証(照合)は、例えば指紋照合の方式では、現状、代表的なものとして次の3方式がある。

①. 指紋の稜線の分岐点、端点の位置と方向を照合するマニーシャア方式。

②. ①に加え、相対的な位置関係を用いるマニーシャアリレーション方式。データ量と処理負荷が大きいが、警察庁が犯人を割り出すのに使用している。

③. 特徴点を含む画像片(チップ)を用いて照合する画像チップ方式。

【0061】方式としての認証精度は、②→③→①の順となっている。また、その各々に対して、どれだけサンプリングするかで照合精度が変化し、サンプリング数を上げると処理時間がかかる。照合精度の取り方としては、例えば、特徴点を15箇所くらい選んで、これを順次照合し、7箇所連続して一致すれば照合作業完了とする。このように特徴点の数と、照合をどこまでで止めるかで照合精度が決まり、例えば全部照合すると時間もかかり、逆に本人照合率が低下することもある。

【0062】基本的に、ライセンスの種類により操縦できる機器が確実に限定されるのが、目標であり理想であるが、上記の問題により認証精度を上げると、処理時間がかかったり、逆に本人でも認証してくれないという現象が発生する。操縦する機器の種類によっては、本人認証のレベルを下げてよいものがあり、処理速度の向上やコストの削減に対応することが可能になる。

【0063】図10の表は、操縦する車種とその重要度とライセンスの資格レベルを示す。重要度はCがもっとも低く、Aがもっとも重要度が高い。また、資格レベルはEがもっとも低く、Aがもっとも高く、高いレベルのライセンスを持つ者は低いレベルのライセンスの運転資格も同時に有する。例えば普通免許証をDとし、原動機付自転車の免許証をEとすると、Dの免許証を持つ者は原動機付自転車の運転も可能である。

【0064】図10の表において、重要度がCの原動機付自転車は、その操縦資格レベルも最低のEであるので、免許証を持っている者ならほとんどの者が操縦可能な機器である。そこで生体認証情報の認証も精密にやる必要がなく、生体認証レベルを最低のレベル「1」としてある。

【0065】普通自動車やタクシー、大型車は、車両のコストも高価で盗難による影響も大きいので、重要度をBとする。その中で普通車は一般個人車両であるので、その資格レベルはD、タクシーは業務車両であるので、その資格レベルをCとする。この2つは、車両の大きさおよび操縦の難易度は同じであるため、生体認証レベルは同じとして、原動機付自転車よりも高いレベル「2」に設定する。

【0066】大型車は、前記2つの車両に比べて大きく、運転も難易度が高いため、より確実な資格が必要(資格レベルB)になるということで、生体認証レベルをさらに高いレベル「3」に設定する。

【0067】そして最後に、緊急自動車は、重要度がAと最も高く、特定の資格者のみが操縦するということで、資格レベルも最高のAとする。そして盗難が発生したときの影響がもっとも大きいので、より確実なドライバーの確認を行うために、生体認証レベルを最高の

「4」とする。この場合、緊急車両は緊急出動が必要と

なるため、確実な認証と同時に、有資格者を間違えずに短時間で確実に認証する必要がある。このため、生体認証のアルゴリズムもそれに適したものを利用することになる。

【0068】図11は、本発明による機器操作権管理システムにおいて、ICカードのメモリ機能を利用して、通行ルートの記録を行う例を示した説明図である。すなわち、図1に示した前記第1実施形態の機器操作管理システムを用いて自動車を運転する者が、その走行経路を自身の記録として、ICカードに保存する方法を示した説明図である。

【0069】図11の(a)は、ドライバーがたどる経路を示している。出発点11040から、道路11030を通過して交差点11020を左折した後、Y字分岐11010を左折して、目的地11000に到着する。この通行経路は、あらかじめカーナビゲーションシステムにより設定しておくが、通行時に、交差点11020の様子を電子カメラで撮影する(11060は、この撮影画像を示している)。画像上に重ねた矢印11070は、実際に自動車が曲がった方向である。

【0070】図11の(b)は、ドライバーの通行経路をドライバーのICカードに記録するフォーマットの例である。通行路を、交差点を主に、いくつかのチェックポイント別に分離し、始点座標と終点座標を緯度・経度で表記し、始点を通過した日付・時刻と、このルートを通行するのに要した時間とを記載する。さらに、交差点のマークとなるように、図11の(a)で撮影した画像のファイル名を添付する。この記録は、走行中に一旦車載の記憶装置に記録して、最後にICカードにダウンロードするようにしてもよい。

【0071】このような記録を行うことにより、ICカード(特にCPUカード)の守秘性により、改変しない正確な走行記録を、走行した個人の管理下に置くことが可能となり、個人的な管理および、例えば同一の車種および外観の自動車が犯罪を起こしたときに、この記録により自身が犯罪とは関係ないことを証明することも可能となる。

【0072】図12は、本発明による機器操作権管理システムにおいて適用可能な、ICカードの機能を自動車の鍵に内蔵した実施形態の例を示す説明図である。

【0073】図12の(a)は、鍵120010にICチップ120020を内蔵させ、インタフェース端子120030によって、この鍵120010と鍵を挿入する自動車の端末とを接続するように構成した例である。この場合、免許証とは形態は異なるが、鍵自身に前述した如くドライバーのID番号や生体認証情報を入れておくことで、現状と同様の鍵の使用のみで、ICカードの利用と同様な効果をもたせることができる。

【0074】図12の(b)は、鍵120011に、図12の(a)の鍵120010の機能に加えて、さらに指紋センサ12

0040を内蔵させた例である。なお、図12の(b)において、120021はICチップ、120031はインタフェース端子である。

【0075】この図12の(b)の例の場合には、鍵120011を自動車の鍵穴に挿入し、ひねってエンジンをかけるという現在の操作とまったく同じ操作で、前記した実施形態と同様の効果を得ることができる。ここで、指紋センサ120040に代替する生体認証情報センサとして、個人によって微妙に異なる指の荷重分布を情報として検出するセンサを用いてもよい。また、荷重分布も面方向だけではなく、鍵をひねる際の時間軸による荷重変化を生体認証情報として用いてもよい。鍵を持つ・ひねるという操作を利用することで、指紋センサという高度なセンサを用いなくても、生体認証情報の認証を行うことが可能である。

【0076】図13は、本発明による機器操作権管理システムにおいて、免許証の種類により運転する車種の限定を行うパターンを示した説明図である。図13の表のフォーマットは、図4、図5と同様のためここでの説明は省略する。

【0077】免許証の種類は練習生、仮免許、本免許、そしてAT(オートマチック車)限定を示す。例えば、教習所内でのみの運転を行う練習生は、エンジン始動も含めてすべて△とする。これは、操作は可能であるが、助手席に本免許証を有するものが搭乗している条件で運転が可能ということを示す。助手席に本免許証を有するものがあることの証明は、教習専用の車で、運転席と同様のICカードリーダーを助手席に設置する方法と、図9で示した運転許可を与えるのと同様に、事前に本免許証を運転席の端末に差し込んで、認証を行った上で、練習生に運転許可を与える方法がある。仮免許による運転許可も同様である。

【0078】本免許は当然すべての自動車の操縦ができるが、ここでAT限定免許の者は、そのライセンスの種類により、AT車の走行は可能であるが、MT車の走行は不可能となる。具体的には、ギアを入れるとスロットルが開かないように、もしくはエンジンストールをするような仕掛けとする。ただし、緊急脱出用にスターターモーターによる走行を可能としたり、5分以内の速度10km/h未満の走行のみを可能とするような制御を行ってもよい。

【0079】図14は、本発明による機器操作権管理システムにおいて適用可能な、端末装置へのICカード挿入時におけるICチップの静電破壊を防止するための、ICカードの実施形態の例を示した説明図である。

【0080】140060は端末(端末装置)側のICカード挿入口であり、挿入時にコネクタ140061にて、ICカード側の電極と接続する。ICカード140000は、その芯が絶縁体で構成され、ICチップ140010が封入されて電極部のみが表面に露出されている。そして、ICカード14

10

20

30

40

50

0000はその周囲を導電体140030が覆っており、導電体とICチップの間にはスパーク等が生じないように一定の間隔があくように、且つ、導電体とICチップとの間にスパークが飛ぶような空間が存在せず、必ず絶縁体がさえぎる形で入るように絶縁体140020の形状が設定されている。

【0081】ICカード140000を利用者が持つと、導電体140030は人体を通じてアースされる(140040)。ICカードを端末に挿入するときに、特に自動車等の場合は、アースに相当する路面との間がゴムタイヤで絶縁されているため、帯電した自動車と挿入したICカードとの間(140070)にスパークが生じる。このスパークがICチップ140010に流れ込まないように、導電体140030を通して人体経由でアースさせることで、端末とICカードの電位を等しくする。また、端末内のICカードスロットには導電ブラシ140050を設け、特にICカードの端子表面の除電や埃の清掃等を行う。これにより、特に自動車特有の高電圧静電気によるICカード(ICチップ)の破損を防止することができる。

【0082】図15は、本発明による機器操作権管理システムにおいて適用可能な、端末(端末装置)とICカード間の情報の守秘を行う実施形態の例を示した説明図である。

【0083】端末150000(端末装置)とICカード150100の間の情報は、例えば図14に示した接点をモニターすることで、傍受が可能である。さらに傍受した信号を解析することで、この接点から擬似的な信号を入力して、ICカード記載事項の変更を行うこともできる。

【0084】そこで、図15に示した本例では、ICカード150100のICチップに、CPU内蔵チップを用い、端末150000との間の信号の授受を暗号化した信号で行う。端末150000側には、ICカードに内蔵したチップと同等の機能を持つCPU内蔵チップ150010、もしくは、専用アプリケーション150020があり、ICカードとの通信をこれらのチップもしくはアプリケーション経由にて行う。ICカード150100に内蔵のICチップと、端末150000側のICチップもしくはアプリケーションは同じ方式による暗号化・復号化機能を有し、ICカード150100の情報の読み出し、書き換え等のコマンドおよび情報の傍受、並びにこれらに基づく変更や偽造を、確実に防止する。免許証番号や氏名等、通常の免許証の記載事項と同等で、秘密にする必要のない情報は、スルー経路150030を通して読み出すことができる。この場合は、例えば電子マネーの残高表示機と同様に、ごく簡単な構造の端末で情報の表示を行うことができる。また、暗号処理を行わなくても、CPUチップの使用により、ICカードへの書き込みアクセスに特定のコマンドを使用することが可能となり、簡便に誤操作や破壊を防止することが可能となる。

【0085】以上、本発明を主として図示した実施形態

によって説明したが、当業者には本発明の精神を逸脱しない範囲で種々の変形が可能であることは言うまでもなく、例えば、ICカードとして接触式で情報を授受するもの以外にも、ICカードに至近距離間での無線送受信が可能な機能を具備させて、非接触で情報を授受するタイプのものを用いることも可能である。この場合、本発明のICチップの機能を、携帯電話や腕時計などの携帯機器に内蔵させることも可能である。

【0086】

10 【発明の効果】以上のように本発明によれば、機器を操作するライセンスとその所有者が同一であることを認証することで、確実な機器操作者の管理を行うことが出来る。また、操作の違反を行った場合の操作制限も、時間軸に沿った木目細かい処理を行うことが出来、より実質に沿った処置をすることが出来る。また、ライセンスのレベルにより、機器操作の制限を細かく設定することが出来、確実な機器操作者の管理と誤操作を防止することが可能となる。さらに、CPUカードを用いることで、物理的な破壊以外のソフトウェアによるカードの破壊を防止しつつ、暗号処理の必要のないデータの簡単な読み出しを可能となる。

【図面の簡単な説明】

【図1】本発明の第1実施形態に係る機器操作権管理システムの構成例を示すブロック図である。

【図2】本発明の第1実施形態に係る機器操作権管理システムにおける、自動車の操縦席近傍へのシステム配置の1例を示す説明図である。

【図3】本発明の第1実施形態に係る機器操作権管理システムにおいて用いる、ICカードの内部構成の1例を示す説明図である。

【図4】本発明の第1実施形態に係る機器操作権管理システムにおける、違反時の罰則処理パターン1例を表で示す説明図である。

【図5】本発明の第2実施形態に係る機器操作権管理システムにおける、ライセンス種類による動作モードの規定の1例を表で示した説明図である。

【図6】本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順の第1例を示すフローチャート図である。

40 【図7】本発明による機器操作権管理システムにおいて、機器を運転する際の操作手順の第2例および第3例を示すフローチャート図である。

【図8】本発明による機器操作権管理システムにおいて適用可能な、ICカードリーダおよび生体認証情報リーダを具備してなる、機器の起動を行うためのリモコンの実施形態の例を示した説明図である。

【図9】本発明による機器操作権管理システムにおいて、機器の使用許可を出していない者に使用許可を出す方法例を示した説明図である。

【図10】本発明による機器操作権管理システムにおい

て、生体認証情報の認証の精度を操縦する機器によって変更するパターンの例を示した説明図である。

【図 11】本発明による機器操作権管理システムにおいて、ICカードのメモリ機能を利用して、通行ルートの記録を行う例を示した説明図である。

【図 12】本発明による機器操作権管理システムにおいて適用可能な、ICカードの機能を自動車の鍵に内蔵した実施形態の例を示す説明図である。

【図 13】本発明による機器操作権管理システムにおいて、免許証の種類により運転する車種の限定を行うパターンを示した説明図である。

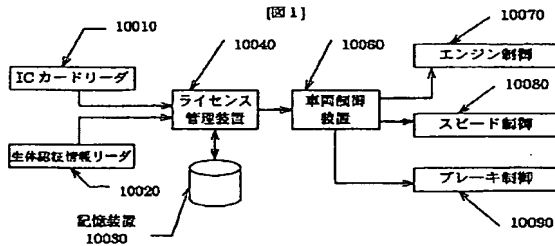
【図 14】本発明による機器操作権管理システムにおいて適用可能な、端末装置へのICカード挿入時におけるICチップの静電破壊を防止するための、ICカードの実施形態の例を示した説明図である。

【図 15】本発明による機器操作権管理システムにおいて適用可能な、端末（端末装置）とICカード間の情報の守秘を行う実施形態の例を示した説明図である。

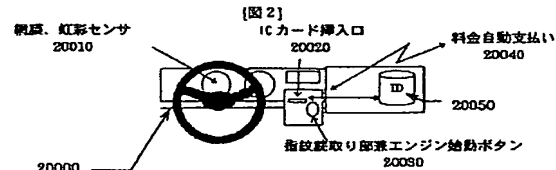
* 【符号の説明】

- 10010 ICカードリーダー
- 10020 生体認証情報リーダー
- 10030 記憶装置
- 10040 ライセンス管理装置
- 10060 車両制御装置
- 10070 エンジン制御装置
- 10080 スピード制御装置
- 10090 ブレーキ制御装置
- 20000 コックピット
- 20010 網膜・虹彩センサ
- 20020 ICカード挿入口
- 20030 指紋読み取り部兼エンジン始動ボタン
- 20040 料金自動支払いシステム
- 20050 記憶装置
- 30000 ICカード
- 30005 ICチップ

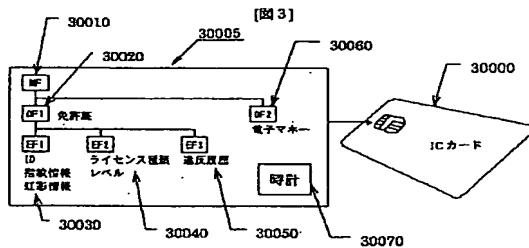
【図 1】



【図 2】



【図 3】



【図 4】

| # | 事項 | 動作モード | | |
|---|----------|-----------|-----------|------------------|
| | | エンジン始動 | 10km/h 未満 | 通常走行 |
| 1 | 無違反 | ○ | ○ | ○ |
| 2 | スピード違反 | ○ | ○ | ○(但 2 日間) |
| 3 | 重大スピード違反 | ○ | ○(但 2 日間) | × |
| 4 | 酒気帯び運転 | ×(但 6 時間) | ×(但 6 時間) | ○(但 5 時間以降 2 日間) |

【図 10】

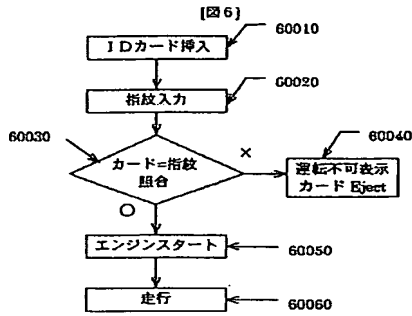
【図 10】

【図 5】

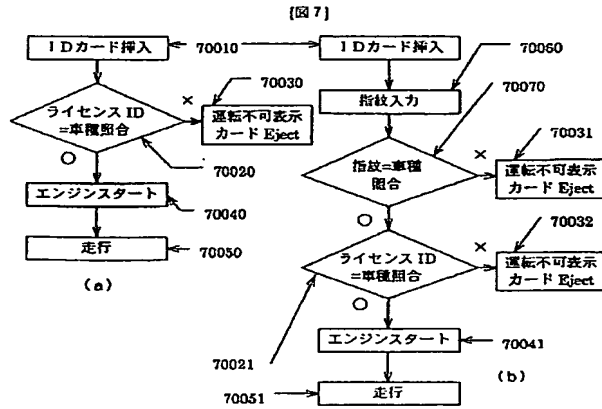
| # | 事項 | 動作モード | | | |
|---|-----------|--------|-------|------|------|
| | | エンジン始動 | ホバリング | 低速飛行 | 高速飛行 |
| 1 | パイロット | ○ | ○ | ○ | ○ |
| 2 | 訓練生 | ○ | ○ | ○ | × |
| 3 | メカニック 1 級 | ○ | ○ | × | × |
| 4 | メカニック 2 級 | ○ | × | × | × |

| # | 事項 | ライセンス管理レベル | | |
|---|---------|------------|-------|---------|
| | | 重要度 | 資格レベル | 生体認証レベル |
| 1 | 原動機付自転車 | C | E | 1 |
| 2 | 普通車 | B | D | 2 |
| 3 | タクシー等 | B | C | 2 |
| 4 | 大型車 | B | B | 3 |
| 5 | 緊急自動車 | A | A | 4 |

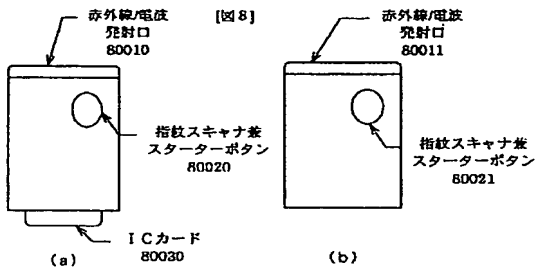
【図 6】



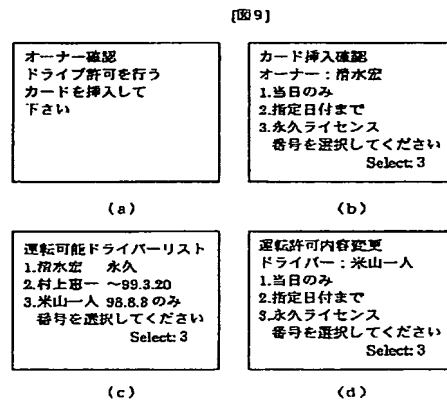
【図 7】



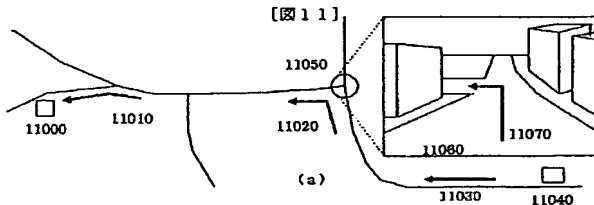
【図 8】



【図 9】



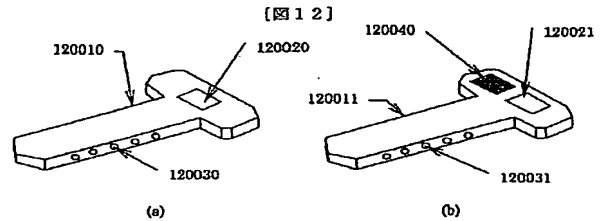
【図 11】



| ルート# | 終点座標 | 始点座標 | 日付 | 時刻 | 所要時間 | 画像ファイル名 |
|------|---------------|---------------|----------|-------|------|-----------|
| 1 | 110.25-540.12 | 111.32-538.00 | H10.7.80 | 14:00 | 8分 | W0001.GIF |
| 2 | 111.32-538.00 | 112.21-535.86 | H10.7.80 | 14:08 | 7分 | W0002.GIF |
| 8 | 120.00-522.65 | 122.37-533.77 | H10.8.2 | 07:59 | 12分 | W0003.GIF |
| 22 | 131.83-525.07 | 130.02-522.95 | H10.8.5 | 16:45 | 15分 | W0022.GIF |
| 23 | 130.02-522.98 | 129.25-521.45 | H10.8.5 | 17:00 | 16分 | W0023.GIF |

(b)

【図 12】

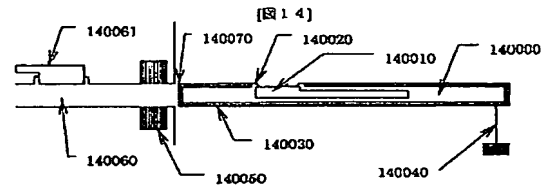


【図 13】

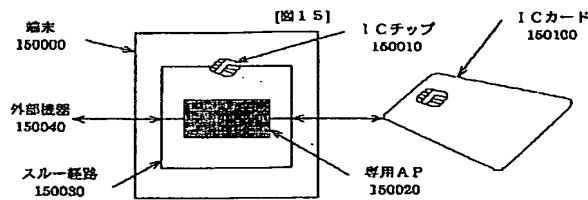
【図 13】

| # | 事項 | 動作モード | | |
|---|--------|--------|-----|-----|
| | | エンジン始動 | M T | A T |
| 1 | 練習生 | △ | △ | △ |
| 2 | 仮免許 | ○ | △ | △ |
| 3 | 本免許 | ○ | ○ | ○ |
| 4 | A T 限定 | ○ | × | ○ |

【図 14】



【図 15】



フロントページの続き

(51) Int. Cl.⁷
G 0 7 F 7/08

識別記号

F I
G 0 7 F 7/08

テーマコード (参考)
A

(72) 発明者 松本 健司
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所デジタルメディア開発本
部内

F ターム (参考) 2C005 MA25 MB01 MB03 MB08 QA01
SA02 SA05 SA15
3E044 AA20 BA04 CA06 CA10 DA05
5B035 AA14 BB09 BC03 CA11
5B043 AA04 AA09 BA02 FA04 GA01
5B058 KA38 YA13